Cybernetics and Battle Management System (BMS) in network soldier system application

Aleksandar Seizovic[a]*, David Thorpe[b],

[a]Engineering Department, University of Southern Queensland, Queensland, Australia; [b]School of Civil Engineering and Surveying, University of Southern Queensland, Queensland, Australia; [c]School of Mechanical and Electrical Engineering, University of Southern Queensland, Queensland, Australia; [d]Rio Tinto Aluminium, Gladstone, Queensland, Australia.

*Corresponding author: Aleksandar Seizovic; Email: acaseizo@gmail.com

Mr. Aleksandar Seizovic
Aleksandar is an Engineers Australia Fellow and an engineering executive who received the Engineers Australia Individual Excellence Award, Queensland, in 2016. He is dedicated to education and is currently engaged in research at the University of Southern Queensland, Australia. His research interests include emergent behavioral phenomena occurring in a system of systems. He is knowledgeable and experienced in business, engineering, and law and is certified to make compliant and governing decisions in business and engineering projects. He has served in the Royal Australian Navy Submarine service and worked in defense, marine, mining, oil and gas, and power generation industries. ORCiD: https://orcid.org/0000-0003-0445-8716.

Dr. David Thorpe
Dr. David Thorpe is an associate professor (engineering/technology management) at the University of Southern Queensland. Prior to joining the university in 2002, he had an extensive civil engineering career in local and state governments, focusing on engineering design, construction, maintenance, and research management in water supply, sewerage, and roadworks. His PhD research from Queensland University of Technology developed a process for managing the physical infrastructure. David teaches life cycle asset management, advanced engineering project management, risk management, related topics, and related engineering management topics to postgraduate engineering students. Additionally, he supervises research projects undertaken by Engineering Honours and Master of Engineering Science students. https://staffprofile.usq.edu.au/profile/david-thorpe; https://orcid.org/0000-0002-5494-7668; OFR: http://dx.doi.org/10.13039/501100001795

Dr Steven Goh
Dr Steven Goh is a seasoned executive, highly credentialed engineer, and highly awarded academic. He has a BEng (Honours) in Manufacturing & Materials from the University of Queensland, MBA (Tech Mgt) from Deakin University, Master of Professional Accounting from the University of Southern Queensland (USQ), Engineering Doctorate from USQ, and Diploma in Company Directorship from the Australian Institute of Company Directors. He is an Engineers Australia Fellow, a Chartered Professional Engineer, and an Engineering Executive, recognised in mechanical engineering and leadership and management. He was awarded the USQ Faculty Award for Excellence in Teaching (Early Career) 2008, USQ Associate Fellow 2009, USQ Senior Fellow 2010, USQ Citation 2010, and the Australian Government's Office of Learning and Teaching (2015) Citation for Outstanding Contribution to Student Learning. He served on the USQ Academic Board, as the 2012 QLD President, a non-executive director of National Board in 2015, Mechanical College Board member, and Congress Member of Engineers Australia. He currently serves as the editor (strategic) for the Australian Journal of Mechanical Engineering and as vice-president of the Australasian Association of Engineering Education. He is the associate head (outreach and engagement) for the School of Engineering at the University of Southern Queensland. https://orcid.org/0000-0002-8583-4586; Scopus Author ID: 27171938400;
Word count: 10700

Cybernetics and Battle Management System (BMS) in network soldier system application

Abstract

Countries use battle management systems (BMS) that enable commands to share digital situational awareness information. The background of the BMS complex system is by Maier definition a system of systems, and current research has focused on distribution of information across a warfighting network. In the network of electronic warfighting platforms where military assets are classified as agents and where multiple subsystems interact, potential permutations and combinations of interactions can cause unpredictable negative or positive feedback loops, resulting in unpredictable or unwanted outcomes, which is referred to as emergence behavior. The Viable Management System is proposed as a governing framework that can be applied in the system where the number of subsystems represents the SoS. The network soldier system is a deterministic system in which behavior is predictable and horizontal recursion is applied to reduce variety. The introduction of stochastics system like cybernetics battle management system (CBMS) is where the system behavior is unpredictable. The CBMS and its application to the network soldier is derived from previous schematics developed by Yolles, Rios, Schwaninger, Lowes, Sisti etc., and the originality is on the aspects of meta-cybernetics and the use of laws of requisite variety by Ashby, 2011.

Keywords: defense; cybernetics; systems; communication; emergence; behavior.

1. Introduction

This paper aims to investigate and review emergent behavior with the system of systems (SoS) structure and function and provide a system within the SoS in an application scenario, namely, “Cybernetics Battle Management System and its Application to the Network Soldier.” Questions arise as to what is the mechanism/process generating emergent behavior in the SoS and what types of emergences are experienced? From a systems perspective, starting with Ashby, emergent behavior is stated to be the lack of understanding of the system. Maier proposed the taxonomy of emergent behavior, and Rainey and Tolk further explored Maier’s taxonomy with the introduction of simple, weak, strong, and spooky emergence and called it the emergence complexity funnel, illustrating emergence behavior in deterministic and scholastic systems. Yolles presented the meta-cybernetics, complexity, and recursion emergence cybernetic schematics, which entail greater complexity that reduces knowability and predictability. Therefore, a system will emerge into the environment in which it exists. In the meta-cybernetics schema by Yolles, the process intelligence (PI) equates to operative intelligence (OI), and as cybernetics orders are coupled together, the systems (meta) with most flexibility will control the system (meta).

This study presents a “real-world application,” which the current literature has not yet addressed.

The contributions of the current study are as follows:

- The requirement for the specification of context, criteria, and a system hierarchical structure in the schematic of the CBMS application to network soldier emergence behavior is outlined.

- Network soldier system variety attenuators and amplifiers to balance variety (haemostatics) use laws of requisite variety (LRV) in dealing with complexity in the environment.
- A schema of system classification is presented to provide the framework in which a network soldier system must be developed in the meta system to explore emergent behaviors in multi-agent systems (O'Toole, Nallur, and Clarke, 2014).

The objective was to demonstrate if any emergent behavior was present in a system (i.e., a complex (multi-agent) system was exhibiting emergence), which can be represented formally using the developed framework (Singh et al., 2017). Then, a modeler could easily analyse and study the causal relationships between the micro and macro layers of a system (Bar-Yam, 2004). Those processes operate according to cybernetic principles and are conceptualized with schematics in the networked soldier's role in a larger SoS such as the battle management system (BMS); there may not be many actual examples available. To be genuinely useful for engineering systems, the schematics must be expanded into at least two fundamental categories: (1) a "discrete" schematic for time-limited operations that terminate, and (2) a "recursive" schematic for extended operations, during a set timeframe, which will not be covered in this study. Further, this study will not cover any form of the distributed battle management (DBM) solution described as disruptive new technology developed to provide timely and relevant information to the battle commander and soldier. The DBM is a semiautonomous software solution used to enable complex teamwork between manned and unmanned platforms in communication-deprived environments.

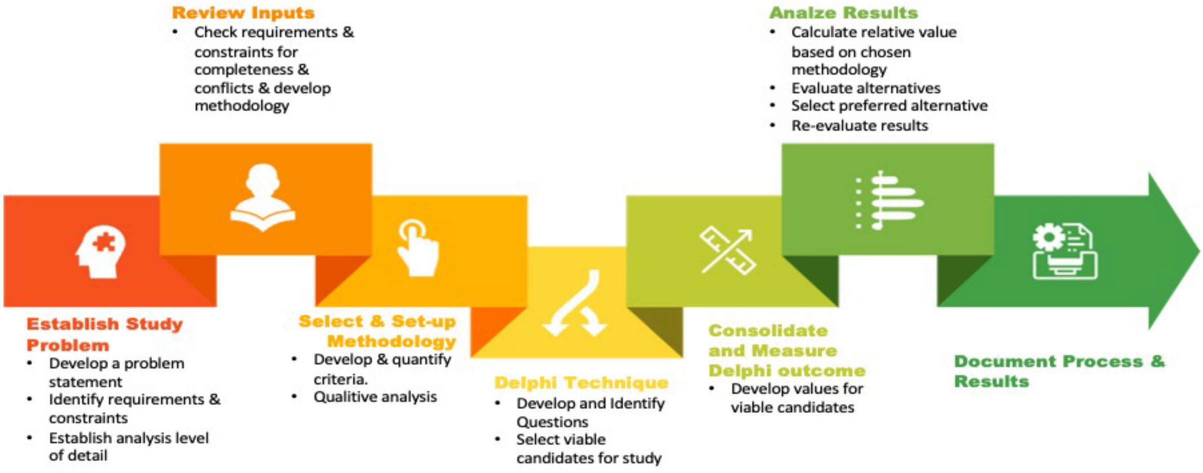
2. Battle management system (BMS)

The Dr Maier SoS definition is referenced in the paper titled, "Emergent Behavior in the Battle Management System (BMS)." Maier, in 1998, described the architecture of a SoS as communication. The architecture is nonphysical and has a set of standards that allow for communication among its components. The SoS and other components of the system are tangible and intangible objects that can be configured such as mechanical, electrical, electronic, software, knowledge, or natural objects. These objects perform functions and behaviors to meet a specified purpose, and they generally fit within the description of emergent behavior as defined in Maier's paper on "Architecting principles for systems-of-systems" (Maier, 1998).

The BMS is an SoS with the mission of defending a continent; it focuses on the distribution of information across a network and is essentially a client-server software. The BMS comprises numerous components such as a tactical computer (TC), local area network (LAN), personal computers (PCs), and servers. A range of servers can be configured for several different platforms. The BMS is a mesh network in which information passes through multiple nodes. Land dismounted soldier wireless networking, sensors, systems, and data communications systems cover a range of wireless networks, integrated power hubs, sensors, end-user devices (EUDs), tactical routers, and network-enabled technologies. Some of these sensors include human biosensors, targeting, shot detection, unmanned aerial vehicles (UAVs), small arms digital sights, and range finders. Because of the complex web of interconnections within the BMS, emergent behavior can occur and cause problems. The aim is to investigate various theories and elements that are and can be relevant to system emergent behavior in a complex SoS. Therefore, the basic theory and research on judgment, decision, and choice are the starting points for the development of a general SoS framework.

3. Research conceptual framework

Conceptual framework (flowchart) that graphically shows the research process



Establish Study Problem
- Develop a problem statement
- Identify requirements & constraints
- Establish analysis level of detail

Review Inputs
- Check requirements & constraints for completeness & conflicts & develop methodology

Select & Set-up Methodology
- Develop & quantify criteria.
- Qualitive analysis

Delphi Technique
- Develop and Identify Questions
- Select viable candidates for study

Consolidate and Measure Delphi outcome
- Develop values for viable candidates

Analze Results
- Calculate relative value based on chosen methodology
- Evaluate alternatives
- Select preferred alternative
- Re-evaluate results

Document Process & Results

Diagram 1: Conceptual framework

4. Literature review including assessment of gaps in existing knowledge

In the literature, many techniques exist to detect emergence, ranging from statistical analysis to formal approaches. For this research, VSM (Ashby 1965, 2011; Chan, 2011; Holland, 2007; O'Toole et al., 2014) is the most appropriate choice to control variety in SoS. The emergent behaviors system comprises of three general elements: agents, their interactions, and the environment. Each agent has a set of attributes that describes the state of the agent and a number of specified policies or rules that define how the agent behaves with respect to the changes in its environment. The SoS objects provide a purpose, and hidden states in various situations in this system can be considered exosystemic (Bronfenbrenner, 2021). The metasystem can be used to explain the hidden states and relationships that occur in a system, while the metasystem can help in explaining any unknown relationship that occurs within (Hundt, 2006 and Djavanshir et al., 2015). This relationship can be generalized to explain a higher order of cybernetics in relation to lower orders (Yolles, 2021).
Various techniques exist to detect emergence (Chan, 2011; Holland, 2007; O'Toole et al., 2014), and the types of conditions are perhaps best evaluated using an emerging strategy (Mintzberg et al., 1998). Some generic examples of failure modes by Meier (2008) observed projects within the U.S. Federal Intelligence and Defense agencies. He discovered a number of particular early warning signs that occurred frequently in these SoSs. SoSs are characterized by unforeseen emergent behavior, and chaotic systems are where the relationships between cause and effect are impossible to determine. Others (e.g., Sheffield et al., 2012; Snowden and Boone, 2007) also referred to complicated and dynamic projects. Complexity comes from interdependencies and uncertainty (Williams, 1999), but also from human-oriented social aspects (Stacey, 2007). Internal complexities, such as technology and interfaces of existing systems, bring particular difficulties in understanding and assessing

project behavior. External complexities such as stakeholder relationships (Pryke & Smyth, 2006), Remington and Pollack (2007) discussed several complexity types and tools to address various elements in complex systems. Other examples of tools include the cause and effective tools that others have developed and used for diagnosing system faults (Williams et al., 1995).

5. Gaps in the literature

- The introduction to systemic thinking and cybernetics and how they provide building blocks of framework elements and methods used in building meta-methodology model is unclear or not available.
- To establish a theoretical framework for modeling and simulation, it is necessary to first establish the taxonomy of emergent behaviors.
- There is no evidence of the emergent behavior present in constituent systems[1] that support systems design. Combinations of systems operating together within a SoS contribute to the overall capabilities. Combining systems can lead to emergent behaviors that may either improve or degrade performance and decrease or increase costs.
- There is no clear understanding of how to test system methodologies while applying system thinking and steer and control theory described as cybernetics, which is the source of knowledge required to mitigate management and operational risk control (Ashby, 1965 and 2011).
- In complex systems, during problem solving, we can assume to have all the systemic properties investigated, and this is when the nature of a problem is indeed revealed. Therefore, cybernetics and system thinking give rise to a new concept in problem solving, which is not well defined and understood in relation to system development (Wiener, 2013).

6. Research methodology design, application, and results

The application of BMS networked soldier scenario is to capture and assess the risks and opportunities of the soldier operations; it is associated with specific sets of elements, particularly where the likelihood of failure occurrences are highly uncertain.

Scenario analysis using the Delphi technique is a system of predicting possible future events by considering possible alternative outcomes. The ideal scenario test is a credible, complex, compelling, or motivating story, the outcome of which is easy to evaluate. What formerly was a simple, top-down system has become a complex bottom-up modeling exercise, involving almost every function within the industries (Beer, 1984, Ashby 1965, 2011).

6.1 Delphi technique

The Delphi technique relies on a panel of experts and is focused on a systematic, interactive forecasting method. This technique consists of a carefully structured ‘scenario pilot test’ with questions, asking participants to provide their view on the application of VMS in meta cybernetics SoS where we can provide control (Davidson, 2014). This will be further analyzed to clearly define the drivers and elements in CBMS control of variety.

The questions will be based on concepts from the pilot test scenario and backed by literature, designed to be asked in any order, allowing the researcher to follow the specific trajectory of the participant’s answers and to explore the emergent themes.

[1] Constituent systems can be part of one or more SoS. Note: Each constituent is a useful system by itself, having its own development, management goals, and resources, but interacts within the SoS to provide the unique capability of the SoS.

- The questions will be emailed to several professionals from organizations based in Australia. These professionals are from academia, military, and defense industry and the assumption is that they will provide similarity in their feedbacks.
- Test methodology by examining how the result of expert opinions compares with drivers/elements.
- What are the drivers, aspects, or elements for decision-making in each of the methodologies?
- From findings, formulate the new model. The system modeling is defined as a construction and development of the frames, rules, constraints, models, and applicable theories, modeling a predefined class of problems (Chang et al., 2014).
- Complete the feedback loop by returning to the new expert panel to test and validate the model (Weiner, 2013).

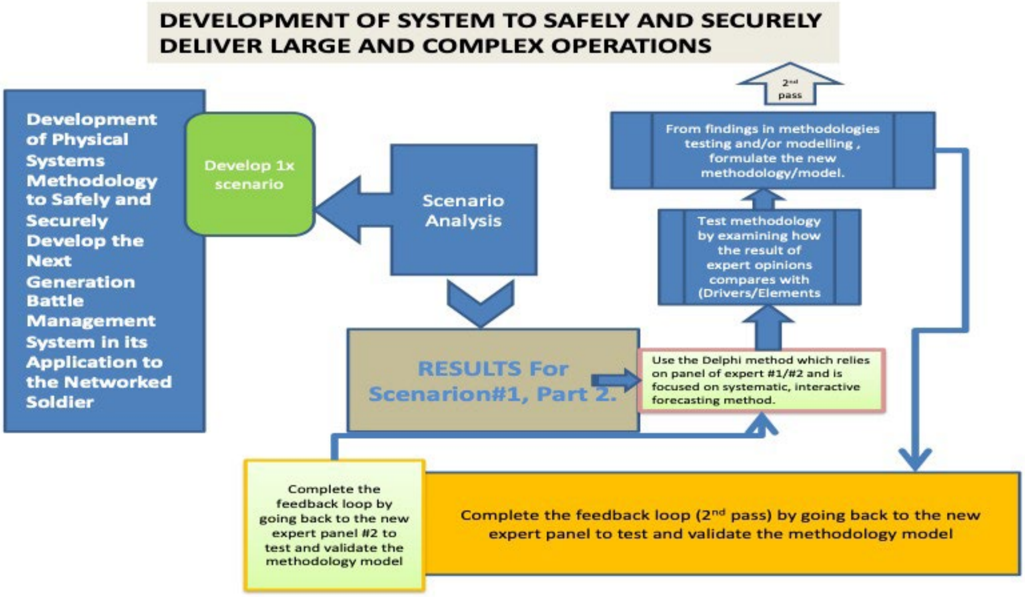

DEVELOPMENT OF SYSTEM TO SAFELY AND SECURELY DELIVER LARGE AND COMPLEX OPERATIONS
2nd pass
Development of Physical Systems Methodology to Safely and Securely Develop the Next Generation Battle Management System in its Application to the Networked Soldier
Develop 1x scenario
Scenario Analysis
From findings in methodologies testing and/or modelling , formulate the new methodology/model.
Test methodology by examining how the result of expert opinions compares with (Drivers/Elements
RESULTS For Scenarion#1, Part 2.
Use the Delphi method which relies on panel of expert #1/#2 and is focused on systematic, interactive forecasting method.
Complete the feedback loop by going back to the new expert panel #2 to test and validate the methodology model
Complete the feedback loop (2nd pass) by going back to the new expert panel to test and validate the methodology model

Diagram 2: Delphi analysis process

7. SoS emergent behavior background

Many authors (cf. Bonabeau et al., 1995; Emmeche et al., 2000; Fromm, 2005; Holland, 2007) agree that the notion of emergence involves the existence of levels in a system. Therefore, emergence can be summarized as a characteristic of a system. Properties appear at the system (macro) level that were not explicitly implemented and arise dynamically from the interactions between entities at the component (micro) level (Sing, 2017). Using Fromm's taxonomy to classify emergent behavior and the development of a suitable framework should provide a platform for simulating and analyzing behaviors in a multi-agent system (Mittal, 2017). To establish the theoretical framework for modeling and simulation, the taxonomy of emergent behaviors must first be established. The most cited works to date that have explored the classification of emergent behaviors are by Sing (2017), Johnson (2016), Holland (2007), Fromm (2005), and Bar-Yam (2004).

8. Summary of supporting publication

The publication examines the emergence of SoS to understand the differences in SoS problems where there are multiple interdependent and interrelated SoSs in project management (Koskela and Howell, 2002; Najmanovich, 2002; Maier, 1998; Packendorff, 1995). The approach considered in this thesis is broader and examines a series of SoS methodologies, which are defined as systems with numerous stakeholders, nonlinearities, multiple interdependencies, and feedback systems. The supporting publications are:

- **Emergent behavior in the battle management system**

Today, more than 30 countries use BMSs that enable commands to share situation awareness information; this study focuses on the distribution of information across a warfighting network. Similar to natural systems in which autonomous agents, such as ants and bees, follow a set of simple rules, a BMS is a network of bases and electronic warfighting platforms that have military assets as agents within the network, guided by the defense doctrine (e.g., rules, policies, procedures, and precedents). The rationale for the workability of such a system is based on each subsystem being reliable when multiple subsystems interact. However, the potential permutations and combinations of interactions can cause unpredictable negative or positive feedback loops, resulting in unpredictable and unwanted outcomes. The results of emergent behavior are unexpected and sometimes unwanted in areas such as intelligence, cybersecurity, weapons on target and wireless networks. Understanding emergent behavior is imperative in developing frameworks to deliver large and complex engineering projects safely and securely, produce new insights, and take practical steps towards improving the success of complex projects.

- **Cyber-physical systems and emergent behavior**

This study aims to understand how and why a meta system can be attacked by cybercrime or espionage agencies and to determine whether a methodology can be developed to minimize this occurrence. A 'cyber-physical system' refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to interact with and expand the capabilities of the physical world through computation and C4I (command, control, communications, computers, and intelligence) is a key enabler for future technological developments. The overall purpose of this study is to find opportunities and research challenges, including the design and development of next-generation aeroplanes and space vehicles, plug in hybrid gas electric vehicles, fully autonomous urban driving, and prostheses that allow brain signals to control physical objects (Ansoff, 1975). The basic design of systems study and the components of systems are the configurations of tangible and intangible objects such as mechanical, electrical, electronic, software, knowledge, or natural objects. These objects perform functions and exhibit behaviors to meet a specified purpose and more or less fit the description of emergent behavior as defined by Maier (2013). Although the objects serve a purpose in their own right, in some situations, there are hidden states where these systems can be considered as exosystemic.

9. Cybernetics automated battle management system

A cybernetic automated BMS (CBMS) is based on an autonomic computing concept (Kopetz et al., 2016). The autonomic paradigm is inspired by the human autonomic nervous system, which handles complexity and uncertainties, and aims to realize computing systems (Johnson, 2016) and applications capable of managing themselves with minimum human intervention (Burbeck, 2007). Challenges are presented to ensure that cyberspace resources and services can effectively tolerate cyberattacks and automatically manage their resources and services (O’Connell, 2012). There are no effective commercial technologies for securing and protecting cyberspace resources and services. This is because they are labor intensive (e.g., patch updates), signature-based, and not sufficiently flexible to handle the complexity, dynamism, and rapid propagation of cyberattacks (O’Connell, 2012). Therefore, any changes in the environment and the operation will lead to a high level of false alarms. The high level of false alarms will make the normal intrusion detection systems ineffective. Most intrusion detection/protection systems that are commercially available today are signature-based and require intensive manual management (Song, Fink, and Jeschke, 2017). The primary reason for failure is that they are either signature-based or anomaly-based solutions that are very simple (e.g., threshold base) and require intensive fine tuning and adjustment. Changes in the environment and work lead to false alarms and make anomaly-based intrusion detection systems ineffective (Song, Fink, and Jeschke, 2017). The online use of smart or intelligent monitoring tools, such as the new smart algorithms, data mining, and statistical and correlation models, is to accurately characterize the normal behavior of cyberspace resources and services. The online smart monitoring tools can detect any anomaly events triggered by attacks, faults, or incidents.

The successful development of CBMS technology in command and battlefield layers will have profound impacts because it will present the following advantages:

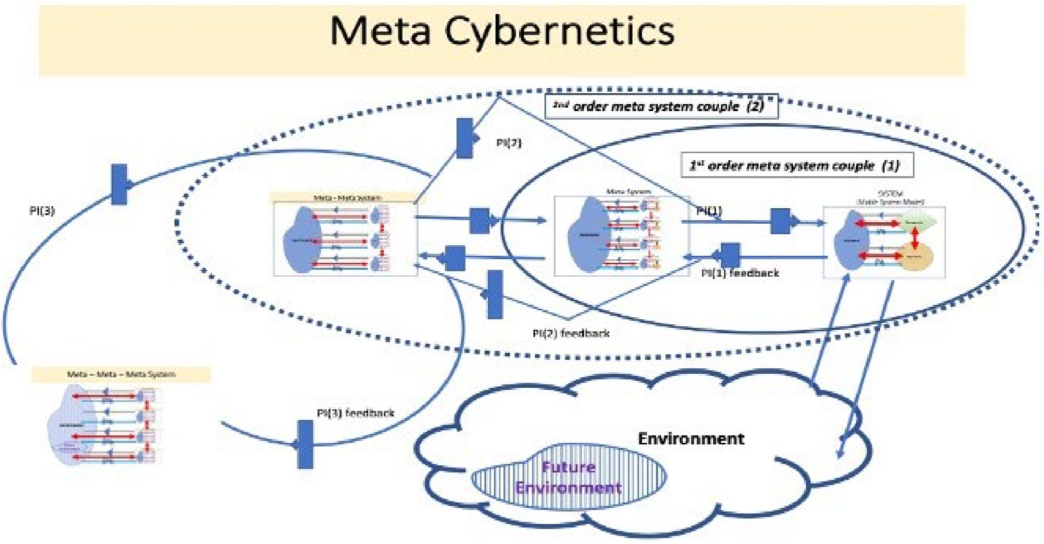
- Stop/eliminate the effectiveness of cyberattacks (known or unknown);
- Deliver uninterrupted services and applications despite, attacks and failures; and
- Build ‘hassle-free’ computing environments that are self-aware, self-adapt, self-heal, and self-protect (Johnson, 2016; Sternberg and Frensch, 1991).

CBMS technology is extremely important for securing and protecting defense networks and services. In this study, we integrate BMS, process, computation, and networking and use embedded computers and networks to monitor and control the networked soldier’s behavior and to combat physiological monitoring systems with feedback loops in which the networked soldier’s behavior and actions can affect computation, and vice versa.

10. Justification of method used

During the Second World War, the mathematician Norbert Wiener (Wiener, 1973) and some respected professionals and colleagues (von Foerster et al., 1955) developed a new branch of applied science and named this science of information feedback systems *cybernetics*. Fourth-order cybernetics is called emergent cybernetics or meta-cybernetics, which considers what happens when a system redefines itself. It implies that a system will “immerge” into its environment, of which it is a part. Particularly, the axioms or elements of systems theories are defined as the centrality, contextual, goal, operational, viability, design, and information. Using cybernetics management (Beer, 1959), this literature review is to examine emergent behavior through the theory of critical system thinking (D’Andreamatteo et al., 2015) and cybernetics methodology. The cybernetics methodology is called the “new paradigm” that has attracted numerous researchers and practitioners and introduced them to the discipline of systematic management.

Meta-cybernetics or fourth-order cybernetics acknowledges the emergent properties of complex systems.



Schematic 1: 4th Order Metasystem (emergent cybernetics) Hierarchy for VSM.

Emergence entails a greater complexity that reduces knowability and predictability. Therefore, a system will immerge itself into the environment in which it exists. Immergence means "submergence" or "disappearance in, or as if in, a liquid." The distributed nature of fourth-order cybernetics is as follows:

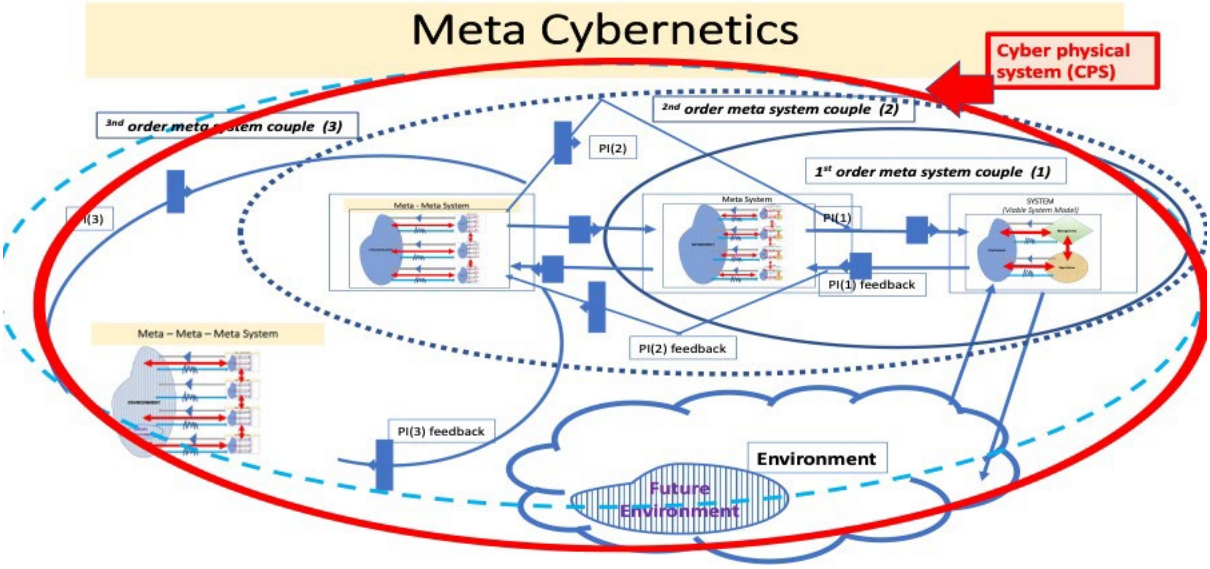
- Who (or what) is capable of seeing a fourth-order system in its full complexity?
- At the fourth order, the discrete observer's boundaries become problematic.
- Who is sufficiently mercurial to notice all relevant changes as and when they occur?
- A single agent is unable to see enough—its standpoint is too fixed, partial, or out of date.

11. Cyber-physical system (CPS) and cybernetics battle management system (CBMS)

Present-day CPSs integrate computational and physical processes to perform various mission-essential or safety-critical tasks (Nweke, Weldehawaryat, and Wolthusen, 2021). The ability to interact with and expand the capabilities of the physical world through computation, communication, control, and computers (C4) is a key enabler for future technological development. Opportunities and research challenges include the design and development of next-generation aeroplanes and space vehicles, electric vehicles, fully autonomous urban driving, and prostheses that allow brain signals to control physical objects. Increased efficiency of either information or data flow alone can change the entire organizational construct within which the system operates. CBMSs have traditionally combined elements of cybernetics, mechatronics, control theory, systems engineering, embedded systems, sensor networks, data, distributed control, and communications (Wiener, 2013). Properly engineered CPSs and CBMS rely on the seamless integration of digital and physical components, as well as the possibility of human interactions, which necessitates reliable C4I.

Increased information and data flow efficiency alters the entire organizational structure within which a system operates. CPSs and CBMS connect cyberspace to the physical world through a network of interconnected elements such as sensors, actuators, robots, and computational engines. These systems are highly automated, intelligent, and collaborative (Nweke, Weldehawaryat, and Wolthusen, 2021). Energy-neutral buildings, zero-fatality highways, and personalized medical devices are all examples of CPSs.

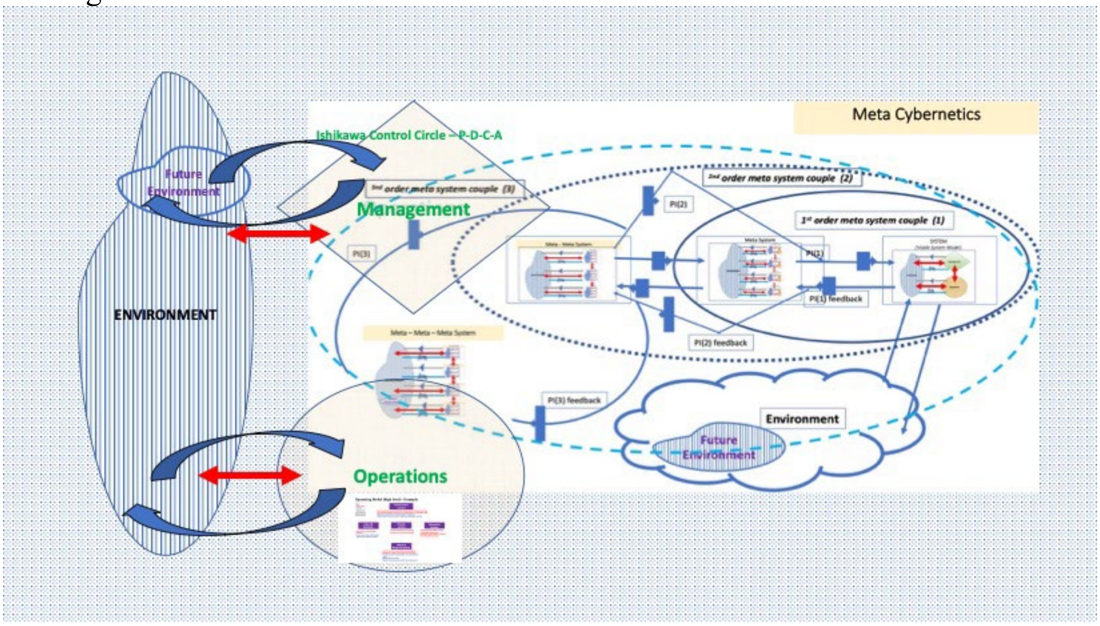
A direction for future research on CPSs is creating standardised abstractions and architectures that permit the modular design and development of CPSs; these are urgently needed. CPSs and cybernetics feedback techniques link cyberspace with the physical world through a network of interrelated elements such as sensors and actuators, robotics, and computational engines (Walsh, 2019). These systems are highly automated, intelligent, and collaborative. Examples of CPSs and cybernetics include energy-neutral buildings, zero-fatality highways, and personalized medical devices. CBMSs require detailed modeling of the dynamics of the environment and a clear understanding of the interactions between the dynamics of the embedded system and its environment (Walsh, 2019). It is important to consider the scenario in which an alert is issued because of a cyber or an electronic warfare attack that has spoofed the system. Therefore, headquarters (HQ) looks at an uncommon BMS program location for something that does not exist; however, another covert operation is being carried out elsewhere (Ward and Chapman, 2011).
Cybernetics began to question the ideas of systems in control and out of control in first and second order behaviors. The Law of Requisite Variety makes it clear that control has limits. When Ashby described first and second order effects, he was not thinking of autonomy or intelligent SoS, though he clearly understood the possibilities of emergent behavior (Ashby, 2011).


Meta Cybernetics
Cyber physical system (CPS)
2nd order meta system couple (2)
3rd order meta system couple (3)
PI(2)
1st order meta system couple (1)
PI(3)
Meta - Meta System
Meta System
SYSTEM (Viable System Model)
PI(1)
PI(1) feedback
PI(2) feedback
Meta – Meta – Meta System
PI(3) feedback
Environment
Future Environment

Schema 2: Meta-Meta Cybernetics and CPS domain

Future effects of the CBMS and Cyber-Physical System (CPS) will have a considerable impact on our personal and professional lives (Song, Fink, and Jeschke, 2017). Autonomous machines and complicated data environments involve legal requirements such as responsibility, liability, data ownership, and privacy (Katz and Ruhl, 2015).

Systems and components of systems are configurations of tangible and intangible objects such as mechanical, electrical, electronic, software, knowledge, or natural objects (System Engineering Body of Knowledge (SEBoK) Editorial Board, 2021; Dyson, 1997). These objects perform functions and behaviors to meet a specified purpose, and they fit within the description of emergent behavior defined by Maier (2014). Although the objects provide a purpose in their own right, situations exist in which there are hidden states where such a system can be considered exosystemic. Thus, a machine SoS exists that must be designed, manufactured, and operated to deliver its purpose (Dyson, 1997). An example of this is a communication SoS (satellites, land stations, submarine cables, and facilities) that enables household and business transactions, manufacturing, the control of autonomous vehicles in mines, or the management of a battlespace. The components of this SoS are systems in their own right.



Schematic 2: Meta-Cybernetics (VSM) in SoS System

For the system to meet its purpose, another complex SoS must be in place (Bar-Yam, 2004): a system of maintenance and support (Dyson, 1997). This additional system has objects, such as human skills, machine learning, performance measures, tools, knowledge, and facilities (Dyson, 1997), and has two main subsystems: social and technical. A social subsystem describes the functions and behaviors that humans apply to a maintenance system (Dyson, 1997). A technical subsystem describes the technological functions and behaviors that deliver the required purpose.

In future conflicts, Australian land forces may have degradation or lack of communications capabilities essential for BMS coordination and situation awareness understanding. Therefore, the introduction of the DBM solution, which is the disruptive new technology, may serve to develop suitable automated decision tools to integrate with BMS command and soldiers. The DBM solution is to develop new algorithms that are reliable and realistic for warfighting environments. The automated BMS will not be considered in this paper. The automated BMS is used to support the human decision-makers. The ABMS is developed to process large amounts of data to develop battlespace knowledge and awareness and identify and prioritize resources and actions.

12. BMS and networked soldier system

The networked soldier system is a system rather than an SoS; thus, it is important to identify the critical set of systems that affect the SoS's capability objectives and understand their interrelationships (Australian Soldier Systems Architecture (ASSA), 2013). The SoS can place demands on constituent systems that cannot be supported by said systems.

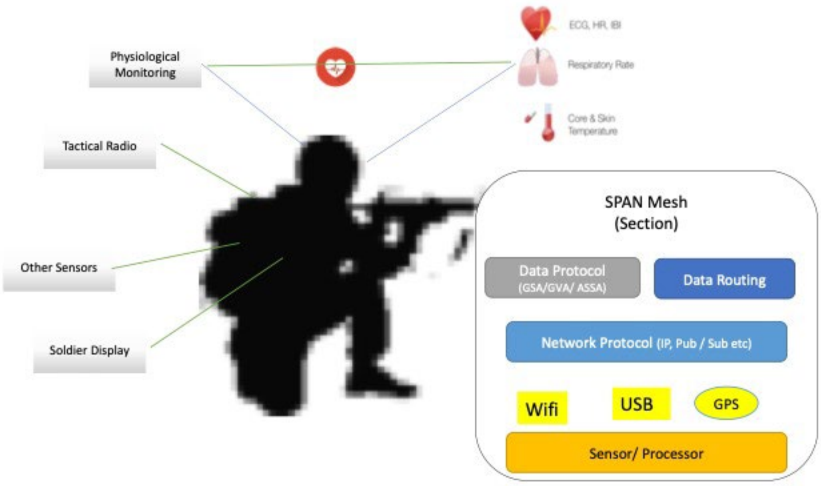
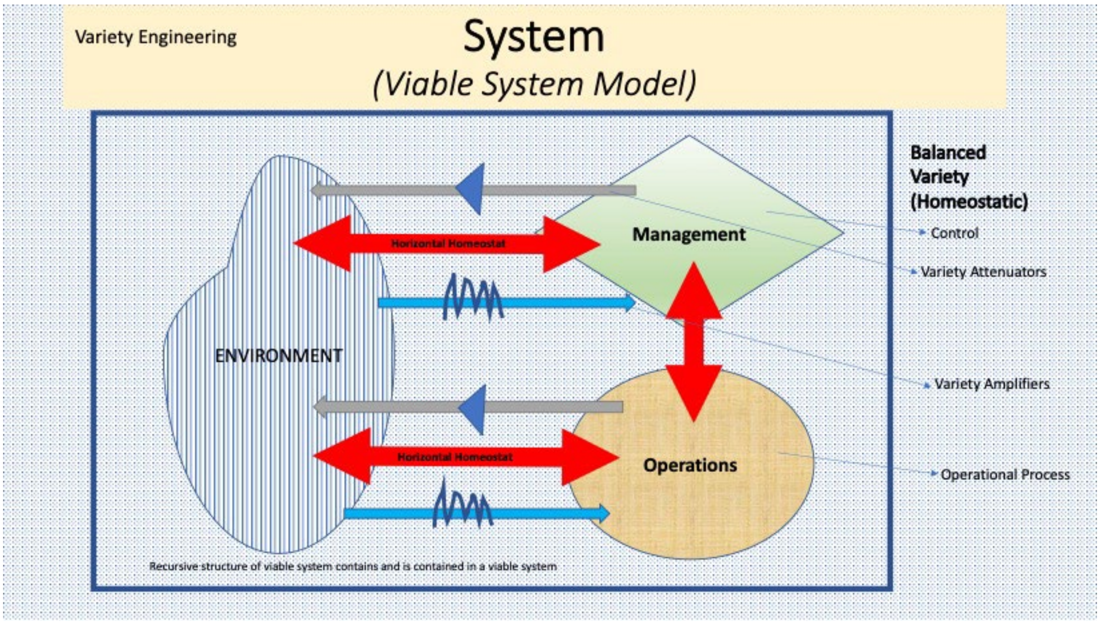


Diagram 3: Network soldier

Combinations of systems operating together and collaborating within the SoS contribute to the overall capabilities. Maier (2014 and 1998) defines managerial and operational independencies, which combine systems and lead to emergent behaviors more than is usual in single systems. These emergent behaviors, as with emergent behaviors of single systems, may either improve or degrade performance (Jackson, 2010). In addition to the ability of the systems to support the functionality and performance called for by the SoS, there can be differences in characteristics between the systems that contribute to the SoS's suitability (Menčík 2016) such as reliability, supportability, maintainability, assurance, and safety (Zio and Sansavini, 2011). The challenge of designing a system is to leverage the functional and performance capabilities of the constituent systems to achieve the desired SoS's capability, as well as its crosscutting characteristics, to ensure the fulfilment of broader user needs (Jackson, 2010).

13. Network soldier as a system

The technological advances that have enabled a new way of using wearable sensors for medical purposes (e.g., temperature, heart rate) can be used to identify whether a soldier is in medical distress. In the past, it was not possible to access this information remotely unless the soldier radioed in and offered the information. With medical information connected to a BMS and tactical network, the soldier's (known as a networked soldier) medical condition can be identified before the soldier may even be aware of it, and an alert may be raised. If an alert is raised on an entire company, the system will 'know' that a stressor of some kind is impacting the soldiers, and that some action is necessary (ASSA, 2013). Smartphone ad-hoc networking (SPAN) and mesh concept design interconnections between devices or nodes are provided. Data from a networked soldier can be used to simulate different scenarios for testing and analysis purposes (Osipov et al., 2018). Data can be used to identify areas where the safety and security of a soldier as a system or subsystem exist (ASSA, 2013).



Schematic 3 - Viable System Model (VSM) single system

The soldier is treated as a system, including everything from batteries to new concepts such as the digital water bottle. The balance between armour and mobility is the sharing potential of a fully integrated infantryman combat system, where commanders at tactical, operational, and strategic levels can continuously monitor the mission in real time. The soldier functions as a sensor and relays vital information directly to the command element from the battlefield (Generic Soldier Architecture (GSA), 2017). Below are some of the key high-level requirements of the network soldier system:

- Soldiers shall be able to input and update the relevant information into the system swiftly and only the essential information shall be shown,
- Information is to be distributed within the squad level network immediately and sometimes automatically,
- Speech and data communications shall be available simultaneously and in real time,
- The system shall have an integrated information security solution suited to the battlefield,
- The system shall have a modular and scalable architecture, and
- The system shall support visual and physical sensors to supply real-time information to the squad leaders.

a. Physiological monitoring

The ability to remotely monitor the physical condition of each soldier in a dismounted unit is an essential component of the safety, efficiency, and effectiveness of the unit. The physiological monitoring system focuses on collecting, storing, and transmitting physiological data from soldiers to commanders. The system comprises a set of wearables (minimally invasive sensors) that collect data and monitor several parameters of the soldier's body, such as electrocardiogram (ECG), heart rate (HR), and core and skin temperature, and an algorithm to collect, correlate, and distribute the data efficiently (ASSA, 2013).

b. User–machine interface

Significant progress has been made in ensuring that the C4I computer and BMS software meet the needs of dismounted soldiers. While the system has operational value for mission planning and situational awareness when on the halt, the current solution provides a limited means for situational awareness while on the move.

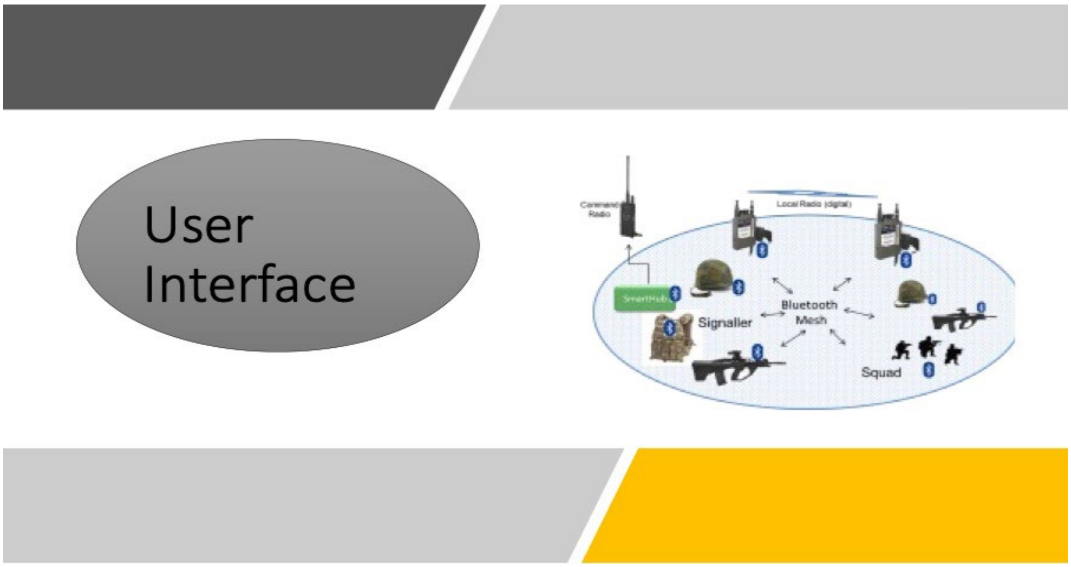


Diagram 4: Soldier User Interface (Elbit Systems Australia)

Additional technologies and solutions, such as voice control, in-ear earphones, and see-through glasses, must be explored to provide a well-rounded solution that can be used during all phases of the dismounted soldier's mission. The soldier system must be sufficiently flexible so that any mix of sensors, processors, user interfaces, and communications can be combined on different fitment locations to create an operational outcome (ASSA, 2013).

14. BMS and network soldier modularity

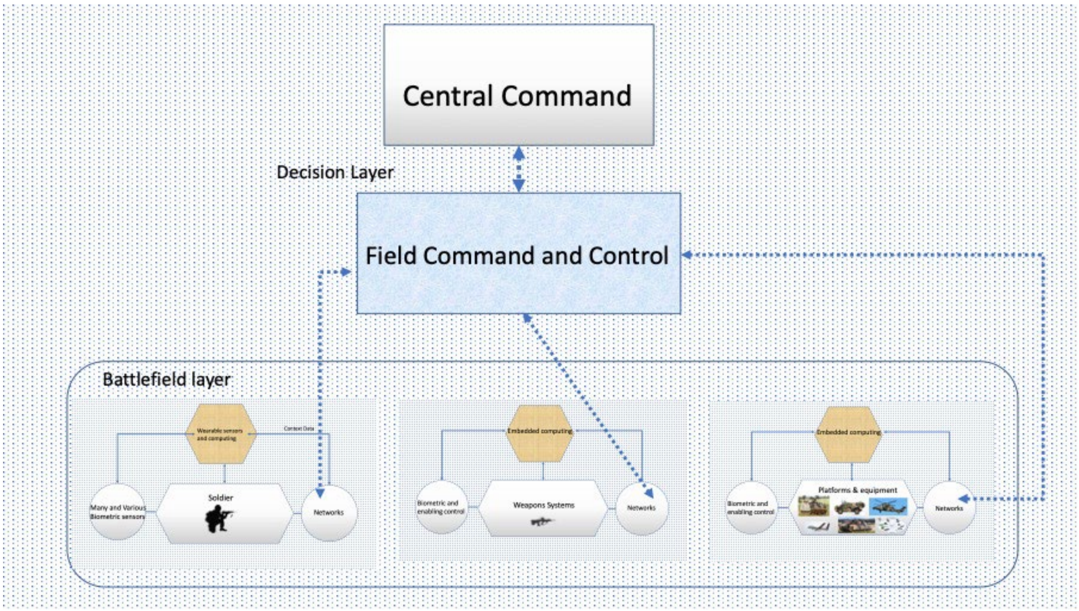
A future soldier system is required to provide an optimized solution for several soldier roles in a variety of mission types. To achieve this, the system must be modular and configurable to support multiple configurations using the same set of building blocks. Its ability to link soldiers in a section and integrate them with the broader land force communication landscape is key to the delivery of SPAN mesh networks (nodes). Networks are now widely seen as the key element in combat, being fitted on a tank, ship, aircraft, or soldier. The network needs to allow for future support of an increasing range of sensors and broader field intelligence capabilities (ASSA, 2013). The SPAN solution is an innovative mesh network for sharing data between soldiers in a section, and between commands and sections. In this study, the mesh network is built on a standardized technology platform and supports a set of standard data exchanges based on generic vehicle (GVA) and generic soldier (GSA) architecture models (Generic Soldier Architecture (GSA), 2017). This allows the SPAN mesh to provide the network for all sensors.

The SPAN mesh at the soldier and section levels is based on leveraging a number of existing wireless technologies with new and evolving technology to create a low-power mesh network such as Bluetooth/Wi-Fi and/or ultra-wide band (UWB). Creating a data standard over a mesh network will allow any sensor, device, or computer to connect as a node and collect or share its data with other nodes in the network. The mesh network's routing capability enables data to flow through the entire section (Generic Soldier Architecture (GSA), 2017). Thus, a dispersed section can continue to share data through links between individual soldiers over a significant distance. Because of the small size, weight, and power (SWAP) of these network components, many sensors can be self-contained and do not require a large separate power supply.

Integrating SPAN with the broader army network is achieved by connecting the SPAN to an existing very high-frequency (VHF) network, broadband, and future waveforms. By combining some existing radio knowledge with the new SPAN mesh and local higher capacity network, a link is created with the land force backbone network. A section commander, signaler, or vehicle can carry the SPAN transceiver and tactical radio to allow this data exchange. With the creation of the SPAN mesh, multiple sensors can be fused to create higher-order information (ASSA, 2013). By connecting sensors via mesh networks to a BMS's processing capability, additional algorithms and techniques can be used to combine and analyze network data (Osipov et al., 2018). Sensors, such as shot and electronic warfare detection and range finders, can be combined to generate information that can be shared across sections and the wider BMS system. Images and videos from local support can be integrated with ranger finders, BMS, and UAV data to create situational awareness (Generic Soldier Architecture (GSA), 2017). The challenge for the modern digital army is the sharing of relevant situational awareness information in and between dismounted teams and outwards to other levels of command and flanking elements (ASSA, 2013).

15. Network soldier system

The network soldier system is an advanced technology program aimed to develop a lightweight and fully integrated infantry combat system. The system will be composed of several subsystems that together shall overcome the limitations that have been identified and have been described in the previous chapter. The program will employ technologies that improve soldier protection, lethality, and situational awareness while at the same time enable reduction of the soldiers fighting load and power requirements.



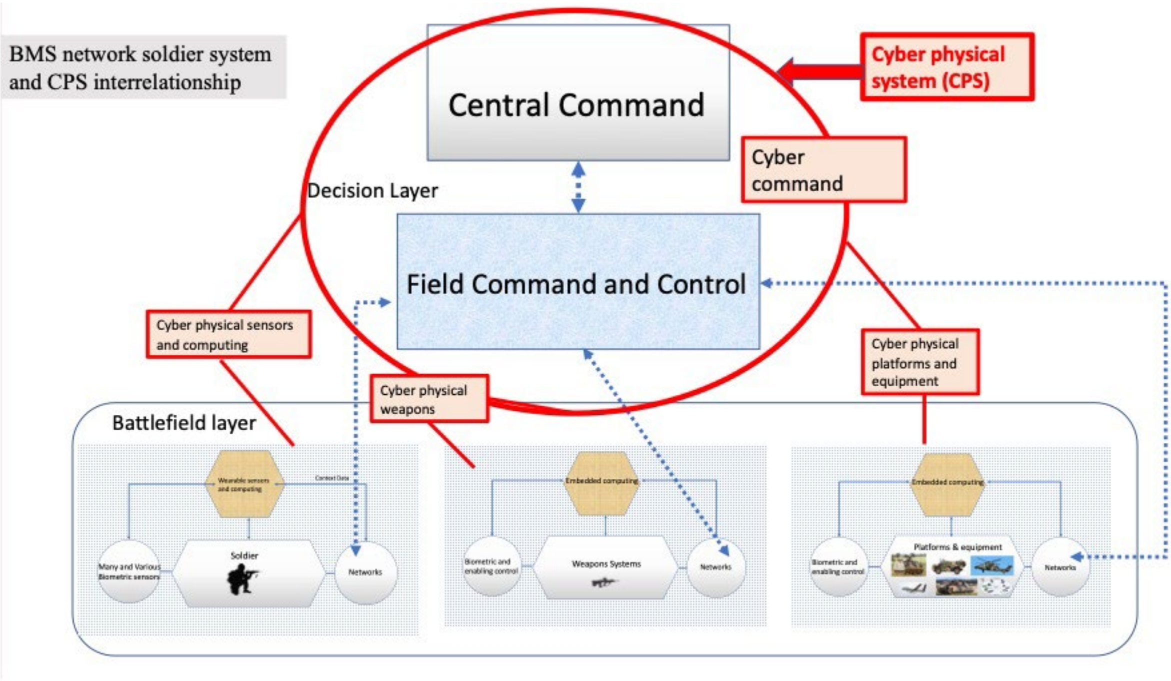
Schematic 4: Command, Battlefield and Computing architecture

During the scenario development, the following areas have been identified as limitations to solutions that are to be addressed in the future solider roadmap:

- Weight, bulk, and cabling of solution affect the manoeuvrability of the dismounted soldier,

- Limited duration of system operation because of energy constraints,
- Limited situational awareness capability when on the move and in active combat because of HMI constraints,
- Lack of Blue Fore Tracking where GPS signal is not available.
- Limited awareness of the physical state of the soldiers in the platoon, and

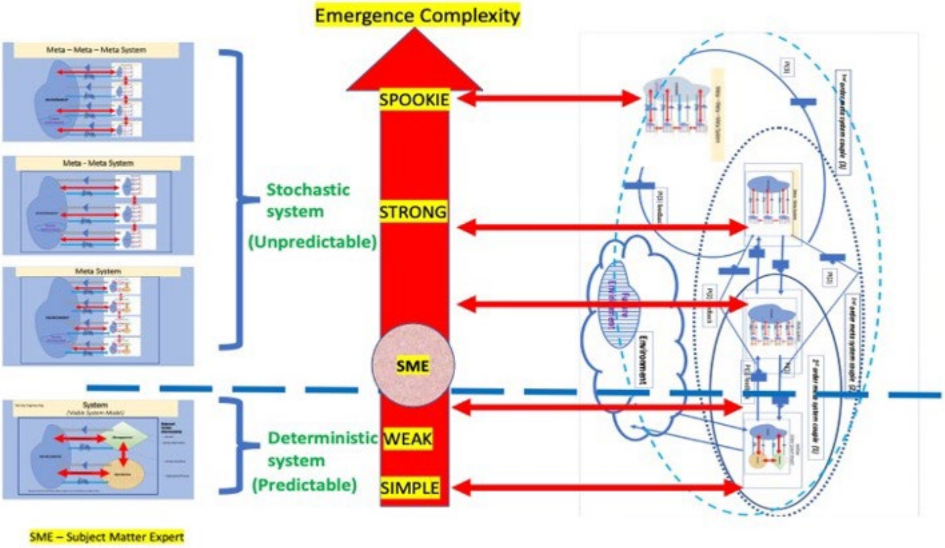
The network soldier system has evolved significantly over the past years and continues to evolve through an ongoing development plan driven by advances in technology together with lessons learned through operational use in the field. The Next-Generation Soldier System is a product of several cycles of evolution, each cycle bringing enhancements and improvements at the component level as well as additional components to address specific needs. The resulting solution, while functional and with distinct operational value, can be significantly enhanced in terms of functionality, performance, and usability though the employment of advanced technologies now available or to be available in the near future.


BMS network soldier system and CPS interrelationship
Central Command
Cyber physical system (CPS)
Cyber command
Decision Layer
Field Command and Control
Cyber physical sensors and computing
Cyber physical weapons
Cyber physical platforms and equipment
Battlefield layer
Wearable sensors and computing
Context Data
Many and Various Biometric sensors
Soldier
Networks
Embedded computing
Biometric and enabling control
Weapons Systems
Networks
Embedded computing
Biometric and enabling control
Platforms & equipment
Networks

Schematic 5: BMS network soldier system and CPS interrelationship

16. What is emergent behavior?

Emergent behavior in SoS performs functions and establishes purposes that do not reside in any component system. These behaviors are emergent properties of the entire SoS and cannot be localized to any component system. The principal purpose of the entire SoS is fulfilled by these behaviors. The SoS engineering applications that meet the definition of an SoS have also been outlined by Maier (2013). Mittal and Rainey developed and described the emergence complexity funnel used to classify simple to spooky emergence in deterministic and stochastic systems complexity. The total behavioral events of the combined systems working alone or collectively must be visible from the strategic requirement of system performance to the implementation of the system to sustain its purpose. The scope of all aspects of SoS involves an indeterminate number of possible emergent behavior events. These can occur at the purpose strategy level or at the purpose implementation level. Emerging behavior should be anticipated even if it cannot be identified in the first instance. Emergent behavior, positive or negative, is an element of systems engineering that should improve both capacity and capability (Dyson, 1997).



Schematic 6: The classification of emergence complexity type (Mittal et al., 2015 and Rainey et al., 2015).

17. Emergence behavior analysis

The method/means technique used for the analysis of emergence in a real-time hostile environment uses graph theory and cognitive science methodology and is applied early in the SoS (Osipov et al., 2018). At this stage, knowledge is independent of experience, and it is difficult to clearly recognise, analyse, and validate where emergent behavior exists; however, it is recommended to use agent-based modeling and simulation to identify the presence of emergent behavior in a BMS (Lee et al., 2018). The presence of emergent behavior in a given SoS application can be proven using agent-based modeling and simulations (Holland et al., 2007). Agent-based modeling is a robust tool for identifying emergent behaviors and clearly demonstrates that emergent behavior does exist in a BMS. Emergent behavior cannot be determined 'through the literature' but through the use of agent-based modeling and simulation, or some other applicable modeling and simulation (M&S) tool, applied to a given SoS engineering application (Lee et al., 2018; Maier, 2014; Maier, 1998). If the presence of emergent behavior is considered to have negative effects, one needs to identify what needs to be done to control it; if the presence of emergent behavior is considered to have positive effects, one aims to identify what needs to be done to capitalize on it.

The complex events used in the analysis of emergent behavior in a multi-agent system are composed of interrelated events, which can be defined at any level of spatio-temporal abstraction. The systems with a large number of components are complex, and their intricate interactions are pervasive (Chen et al., 2014). Examples include natural systems that range from animal flocks to socio-ecological systems and leading-edge engineering (artificial) systems such as the internet and social networks. These systems called complex adaptive systems (CAS) exhibit behaviors from non-linear spatio-temporal interactions among a large number of components and subsystems and are used in data analysis (Kaisler and Madey,

2009) where data is collected across both space and time. These interactions may lead to properties that are often called emergent ones and cannot be derived from those of individual components. Numerous attempts to define emergence have been documented (Holland, 2007). However, a generally agreed upon definition is still lacking. Many authors, such as Singh et al. (2017), Johnson (2016), Holland (2007), Fromm (2021), and Bar-Yam (2004a), have agreed that the notion of emergence involves the existence of levels in the system. Therefore, emergence can be summarized as a characteristic of a system. In this manuscript, we are addressing the issue of emergent behavior in SoS.

a. Scenario: BMS network soldier creation

The challenge for the modern digital army is the sharing of relevant situational awareness information in and between dismounted teams and outward to the other levels of command and flanking elements. The growth of new technology and miniaturization of sensors, such as laser range finders, UAVs, and night vision means that significant advantage can be gained by sharing the relevant acquired information via images or tagged data directly to command, section, or soldier.

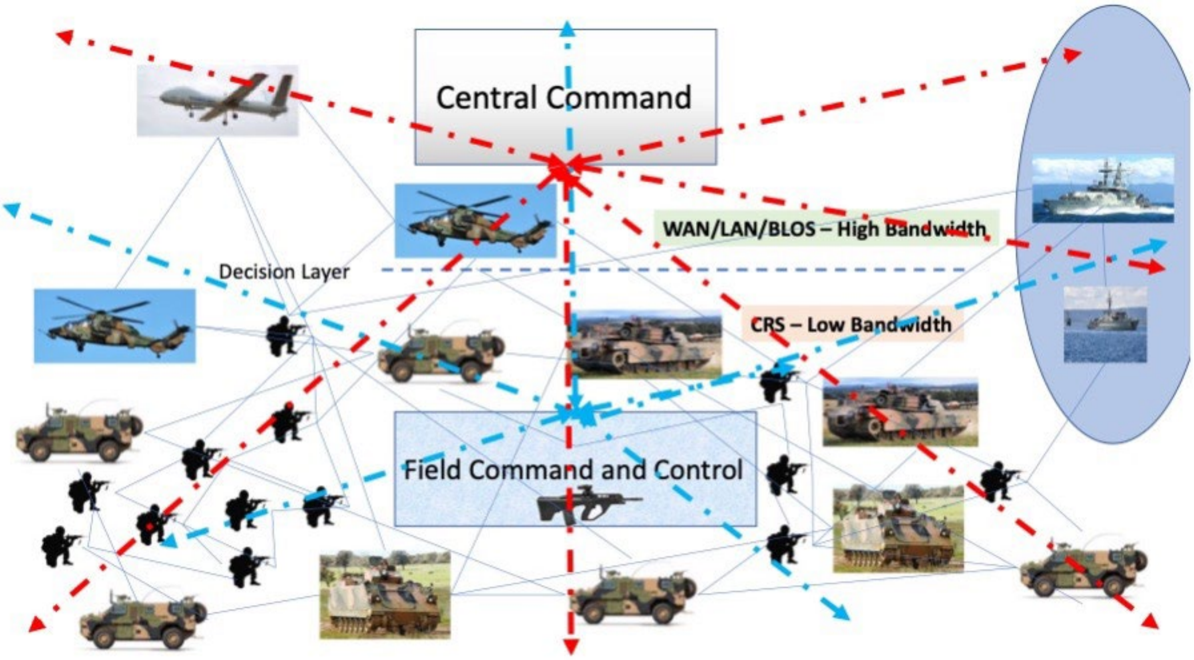
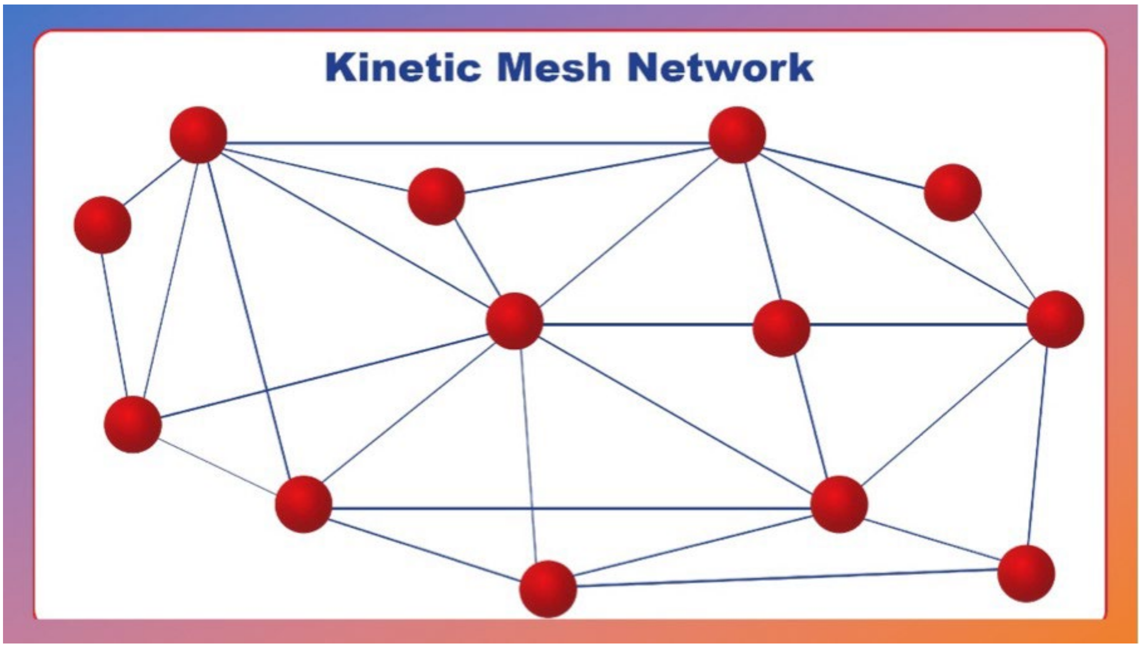


Diagram 5: Example of BMS Communication Network (Elbit System Australia)

The kinetic mesh technology can be used in many applications where infrastructure devices are constantly moving in a rugged environment similar to defense land forces.



Schematic 7: Example Kinetic Mesh Network

18. Pilot test scenarios and test case

The Pilot test is captured in (Annex A and Annex B)

Purpose of Pilot

- The primary purpose of the Pilot was to verify that the cybernetics BMS network soldier scenario developed in this paper for model design, analysis and integration of BMS, process, computation, and communication networking is valid.
- The secondary purpose was to use the lessons learned from the Pilot to confirm that embedded computers and communication networks control the networked soldier behavior and combat the physiological monitoring system (feedback loops) in which the networked soldier's behavior and actions can affect computation and vice versa.

Scope of Pilot

- The Pilot tested the CBMS SoS emergent behavior related to the CBMS network soldier in the battlefield environment. The specific areas chosen for this Pilot test are only in the areas of the BMS platform and system integration, site configuration, unit data manager, and network management. The soldier is a 'system' and integrated within the BMS 'SoS'. The application of (cybernetics is deterministic 'system') viability is controlled through LRV. In SoS, the application of cybernetics is described as meta-cybernetics. The summary of this modeling is based on validating this Pilot test, and the BMS emergent behavior theory is supported by literature.

19. BMS network soldier conceptual model observations

The challenge for the modern digital army is the sharing of relevant situational awareness information in and between dismounted teams and outward to the other levels of command and flanking elements. The growth of new technology and miniaturization of sensors, such as laser range finders, UAV's, and night vision means that a significant advantage can be gained by sharing the relevant acquired information via images or tagged data directly to command, section, or soldier. The networked soldier is a good scenario model for design and analysis because of the integration of BMS, process, computation, and networking, where embedded computers and networks can monitor and control the networked soldier behavior and combat the physiological monitoring system with feedback loops in which networked soldier behavior and actions can affect computation and vice versa.

a. How does the emergent behavior manifest itself?

The SoS, in this case, is a network of bases and electronic warfighting platforms (Lee et al., 2018), and has military assets as agents within the network that are guided by a defense doctrine (e.g., rules, policies, procedures, and best practice). Although each subsystem is reliable, when multiple subsystems interact, potential permutations and combinations of interactions can cause unpredictable negative or positive feedback loops, resulting in unpredictable or unwanted outcomes (Chen et al., 2011). A BMS function and performance specification (FPS) is developed by the defense for the contractor and is defined and validated by a set of requirements (ISO/IEC/IEEE International Standard 2011) for the BMS material systems (Syamil, Doll, and Apigian, 2004). ‘The FPS can identify the start of emergent behavior manifesting in a system or SoS’ (Lee et al., 2018).

b. What are the physical results of the presence of emergent behavior?

The physical results of the presence of emergent behavior in a BMS are goal-seeking elements that may exhibit probabilistic unanticipated behavior. This is because of a set of input conditions that were unanticipated by system software engineers or from the adaptation of a person or software agent to sets of input rules such as misapplication of the rules by a person (Lee and Miller, 2004). Emergent behavior occurs because of the complex web of interconnections within a BMS (Mittal et al., 2015 and Rainey et al., 2015).

c. What are the implication(s) for the existence of the presence of emergent behavior?

Emergent behavior results are unexpected and sometimes unwanted in areas of intelligence, cyber security, weapons on target, wireless networks, integrated power hubs, sensors, EUDs, tactical routers, and network-enabled technologies (O’Connell, 2012). Enabling technologies, such as networks and graphs, are collections of first-person shooter
(FPS) elements (nodes, vertices) and their pairwise links (edges, connections) and are presented in the simple form of a connection matrix showing positive or negative unexpected emergent behavior. This can be analyzed from the perspective of graph theory and cognitive science methodology (Adams et al., 2014).

d. When does emergent behavior occur/arise?

The BMS software in a battlefield environment allows participants to successfully combine and analyze network data with more sophisticated algorithms and techniques than in an operational environment (Lee et al., 2018). Emergent behavior occurs in the communication system interface and in the configuration of the combat network in land dismounted wireless networking, sensors, systems which include human biosensors, targeting, shot detection, UAVs, small arm digital sights, range finders, and data (Singh et al., 2017).

20. Conclusion

A BMS focuses on distributing information across a warfighting network and is a network of bases and electronic warfighting platforms. In this paper, we outlined a framework to explore emergent behaviors in a multi-agent system (O'Toole, Nallur, and Clarke, 2014) and provided insight into the existence of emergence behavior in CBMS by applying the Delphi technique, simple modeling, and referring to the literature.

The objective was to demonstrate the existence of emergent behaviors in a system, for example, a complex (multi-agent) system exhibits emergence and can be represented formally using the developed framework (Singh et al., 2017). This would make it easy for a modeler to analyze and study the causal relationships between the micro and macro layers of a system (Bar-Yam, 2004). It is possible to use a case study to demonstrate how the BMS framework can be useful in implementing and classifying emergent behaviors using existing and known approaches in the literature (Singh et al., 2017). This can be done via system modeling, which includes the analysis, construction, and development of frames, rules, constraints, models, and theories applicable to predefined classes of problems. These methods are critical for effective risk management (Ward and Chapman, 2011). The CPS's involvement in an SoS's emergent behavior necessitates detailed modeling of the environment's dynamics as well as a clear understanding of the interactions between the dynamics of the embedded system and its environment. Maier (2009) defined an SoS's architecture as "communications among components."

The challenge in designing an SoS is leveraging the functional and performance capabilities of constituent systems to achieve the desired capability (Juli, 2011). To establish a theoretical framework for M&S, a taxonomy of emergent behaviors in a project, which is not always clear, must be first established (Mingers and Brocklesby, 1997).

The studies outlined in this paper examined emergent behavior in BMS and vis-à-vis cyber-physical systems (Singh et al., 2017) and make a significant contribution to the literature because they offer insights into a domain that has not been examined in as much depth or detail thus far; valuable additions to the literature can be useful in shaping future research and policymaking in the domain. Furthermore, these papers will be of interest because they present path-breaking and epoch-making contributions to the literature and have the potential to expand the scope of the extant literature on defense.

21. Funding

This work was supported by a postgraduate research scholarship from the University of Southern Queensland.

22. Disclosure statement

The authors report that there are no competing interests to declare.

23. References

Adams, Kevin M., Patrick T. Hester, Joseph M. Bradley, Thomas J. Meyers, and Charles. B. Keating. 2014. "Systems Theory as the Foundation for Understanding Systems." *Systems Engineering* 17 (1): 112–123. doi:10.1002/sys.21255.

Ashby, Ross W. 1965, 2011. *Introduction to Cybernetics*. London: Chapman & Hall, Ltd.

Bar-Yam, Yaneer. 2004. "Multiscale Variety in Complex Systems." *Complexity* 9 (4): 37–45. doi:10.1002/cplx.20014.

Bar-Yam, Yaneer. 2004. *Making Things Work: Solving Complex Problems in a Complex World*. NECSI-Knowledge Press.

Beer, Stafford. 1984. "The Viable System Model: Its Provenance, Development, Methodology and Pathology." *Journal of the Operational Research Society* 35 (1): 7–25. doi:10.1057/jors.1984.2.

Burbeck, Steve. 2007. *Complexity and the Evolution of Computing: Biological Principles for Managing Evolving Systems*. doi:10.13140/RG.2.1.3021.0722.

Chen, Xiangyong, Yuanwei Jing, Chunji Li, and Xiaoping Liu. 2011. "Optimal Strategies for Winning in Military Conflicts Based on Lanchester Equation." *Control and Decision* 26 (6): 946–950.

Chen, C.-C. and Nagl, S. and Clack, C, (2007) Specifying, detecting and analysing emergent behaviours in multi-level agent-based simulations. In: Wainer, G.A., (ed.) Proceedings of the 2007 summer computer simulation conference. Society for Computer Simulation International, San Diego, US, pp. 969-976. ISBN 1565553160. 969-976. 10.1145/1357910.1358062.

"Generic Soldier Architecture (GSA) – MODUK – DEF STAN 23–012." 2017 - Generic Soldier Architecture (GSA). *DEF STAN.* https://standards.globalspec.com/std/10158433/def-stan-23-012. Vols. 23–012, Revision I2.

Darbyshire, Paul & Abbass, Hussein & Barlow, Michael & McKay, Robert. (2000). A prototype design for studying emergent battlefield behaviour through multi-agent simulation.

Elbit Systems Australia Pty Ltd 2020, Copyright approval

Henshaw, Mike. 2015. "Good Practice in Systems of Systems Engineering (SoSE)." In SCI276 Lecture *Series*. CSO, North Atlantic Treaty Organization.

Holland, Orgal T. 2007. “Taxonomy for the Modeling and Simulation of Emergent Behavior Systems Paper presented at the.” 2007. *Spring Simulation Multiconference* 2 Norfolk, March 25–29. doi:10.1145/1404680.1404684.

“IEEE/ISO/IEC 29148-2011 – ISO/IEC/IEEE International Standard – Systems and Software Engineering – Life Cycle Processes—Requirement’s Engineering”. https://standards.ieee.org/standard/29148-2011.html.

Jackson, Michael C. 2010. “Reflections on the Development and Contribution of Critical Systems Thinking and Practice.” *Systems Research and Behavioral Science* 27 (2): 133–139. doi:10.1002/sres.1020.

Johnson, Brian R. 2016. “Design Computing: An Overview of an Emergent Field.” *Bew York*. Routledge.

Kaisler, Stephen H., and Gregory Madey. 2009. “‘Complex Adaptive Systems: Emergence and Self-organisation.’ Tutorial Presented at HICSS-42”. Accessed Jan 5, 2009. http://www3.nd.edu/~gmadey/Activities/CAS-Briefing.pdf. HI: Big Island USA.

Katz, Daniel M., and JB. Ruhl. 2015. “Measuring, Monitoring and Managing Legal Complexity.” *Iowa Law Review* 191. https://scholarship.kentlaw.iit.edu/fac_schol/865.

Kopetz, Hermann, Andrea Bondavalli, Francesco Brancati, Bernhard Frömel, Oliver Höftberger, and Sorin Iacob. 2016. “Emergence in Cyber-Physical Systems-of-Systems (CPSoSs).” Systems of Systems 10099. *Lecture Notes in Computer Science*: 73–96. doi:10.1007/978-3-319-47590-5_3.

Lee, Bengee, and James Miller. 2004. “Multi-project Software Engineering Analysis Using Systems Thinking.” *Software Process: Improvement and Practice* 9 (3): 173–214. doi:10.1002/spip.204.

Lee, Jaeyong, Sunwoo Shin, Moonsung Park, and Chongman Kim. 2018. “Agent-Based Simulation and Its Application to Analyse Combat Effectiveness in Network-Centric Warfare Considering Communication Failure Environments.” *Mathematical Problems in Engineering* 2018: 1–9. doi:10.1155/2018/2730671.

Maier, Mark W. 2009. *The Art of Systems Architecting*. CRC Press.

Maier, Mark W. 2013. “Architecting Principles for Systems-of-Systems.” *Systems Engineering: Journal of the International Council on Systems Engineering* 1 (4): 267–284. doi:10.1002/%28SICI%291520-6858%281998%291%3A4<267%3A%3AAID-SYS3>3.0.CO%3B2-D.

Maier, M. W. 1998. “Architecting Principles for Systems-Of-Systems.” Systems Engineering 1 (4): 267–284. doi:10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D’

Maier, Mark W. 2014. Chap. 2. “The Role of Modeling and Simulation in System of Systems Development” In *Modeling and Simulation Support for System of Systems Engineering Applications*, edited by Larry. B. Rainey, and A. Tolk, 11–41.

McCulloch, Warren S. 1995. “‘Summary of the points of agreement reached in the previous nine conferences on cybernetics.’ Cybernetics: Circular-Causal and Feedback Mechanisms in Biological and Social Systems.” Transactions of the 10th Conference on Cybernetics Ed. H. Von Foerster, M. Mead and H. L. Teuber. New York, 69–80. Josiah Macy Jr. Foundation.

Menčík, Jaroslav. 2016. “Reliability of Systems” In *Concise Reliability for Engineers*, edited by Jaroslav Mencik. doi:10.5772/62358. London: IntechOpen.

Miller, Roger, and Donald R. Lessard. 2008 Chap. 8. “Evolving Strategy: Risk Management and the Shaping of Mega-projects” In *Decision-Making on Mega-projects: Cost–Benefit Analysis, Planning and Innovation*, edited by Hugo Priemus, Bent Flyvbjerg, and Burt van Wee, 145–172. Cheltenham: Edward Elgar Publishing Limited.

Mingers, John., and John Brocklesby. 1997. “Multimethodology: Towards a Framework for Mixing Methodologies.” *Omega* 25 (5): 489–509.

MITRE. 2021. *Treating System of Systems as Systems* MITRE. Accessed December 2021. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-of-systems/treating-systems-of.

Mittal, Saurabh and Larry Rainey. 2015. “Harnessing Emergence: The Control and Design and Emergent Behavior in System of Systems Engineering” In *SummerSim: Summer Simulation Multi-Conference.* Vol. 2015. Chicago, 26-29 July, 2015.

Nweke, Livinus O., Goitom K. Weldehawaryat, and Stephen D. Wolthusen. 2021. “Threat Modelling of Cyber–Physical Systems Using an Applied π-Calculus.” *International Journal of Critical Infrastructure Protection* 35: 100466. doi:10.1016/j.ijcip.2021.100466.

O’Connell, Mary E. 2012. “Cyber Security without Cyber War.” *Journal of Conflict and* Security Law 17 (2): 187–209. doi:10.1093/jcsl/krs017.

Osipov, Yu S., and V. I. Maksimov. 2018. “Tracking the Solution to a Nonlinear Distributed Differential Equation by Feedback Laws.” Numerical Analysis and Applications 11, 158–169. doi:10.1134/S1995423918020064.

O’Toole Eamonn, Vivek Nallur, and Siobhan Clarke. 2014. “Towards Decentralised Detection of Emergence in Complex Adaptive Systems.” Vol. 2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems, 60–69. doi:10.1109/SASO.2014.18.

Polanyi, Michael, and Rainer Tod Allen. 1997. “Society, Economics and Philosophy” In *New Brunswick NJ: Transaction Publishers*, edited by Larry B. Rainey, and Andreas Tolk 2015. *Modeling and Simulation Support for System of Systems Engineering Applications.* Hoboken: John Wiley & Sons, Inc.

Rainey, Larry B., and Mo. Jamshidi. eds. 2019. *Engineering Emergence: A Modeling and Simulation Approach*. Boca Raton: CRC Press.

Rainey, Larry B and Andrew G. Loerch. eds. 2007. “Methods for Conducting Military Operational Analysis.” *Military Operations Research Society and LMI Research Institute*.

Rainey, Larry B., and Andreas Tolk. eds. 2015. *Modeling and Simulation Support for System of Systems Engineering Applications*. Hoboken: John Wiley & Sons, Inc.

Sage, Andrew. P. 2016. “Cybernetics and Complex Adaptive Systems.” In *Encyclopedia of Operations Research and Management Science*, edited by Saul I. Gass, and Michael C. Fu. Boston, MA: Springer. doi:10.1007/978-1-4419-1153-7_205.

Schwartz, Shalmon. H. 2012. “An Overview of the Schwartz Theory of Basic Values.” *Online Readings in Psychology and Culture* 2 (1). doi:10.9707/2307-0919.1116.

Singh, Shweta, Shan Lu, Mieczyslav M. Kokar, Paul A. Kogut, and Martin L, 2017. "Detection and Classification of Emergent Behaviors Using Multi-agent Simulation Framework." Proceedings of the Symposium on Modeling and Simulation of Complexity in Intelligent, Adaptive and Autonomous Systems. Accessed Apr 23–26. https://dl.acm.org/doi/abs/10.5555/3108414.3108417 Paper presented at MSCIAAS'17. Virginia Beach, VA.

Song, Houbing, Glenn, A. Fink, and Sabina Jeschke. 2017. "Legal Considerations of Cyber‐Physical Systems and the Internet of Things" In *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*: 93–115. doi:10.1002/9781119226079.ch5.

Stephenson, Peter R. 2017. "Defining a Cyber Jurisprudence." Paper presented at the Annual ADFSL Conference on Digital Forensics, Security and Law, Florida, May 15 and 16.

Sternberg, Robert J., and Peter A. Frensch, eds. 1991. *Complex Problem Solving: Principles and Mechanisms*. Hillsdale, NJ: Lawrence Erlbaum.

Syamil, Ahmad, William J. Doll, and Charles H. Apigian. 2004. "System Performance in Product Development: Measures and Impacts." *European Journal of Innovation Management* 7 (3): 205–217. doi:10.1108/14601060410549892.

"Australian Soldier Systems Architecture." 2013 (ASSA) for Land 125 Phase 4. https://www.systematiq.com.au/2017/07/03/development-of-australian-soldier-systems-architecture/.

Thomann, James, 1973. "Meta-methodology: An Overview of What It Is and How It Was Developed." Paper presented at the 58th American Educational Research Association Annual Meeting, New Orleans, Louisiana, February 26 – March 1.

Walsh, Melany 2019. "How to Best Protect Military Industrial Control Systems from Cyberattacks." https://www.fifthdomain.com/opinion/2019/08/01/how-to-best-protect-military-industrial-control-systems-from-cyberattacks/.

Ward Stephen and Chris Chapman. 2011. *How to Manage Project Opportunity and Risk: Why Uncertainty Management Can Be a Much Better Approach than Risk Management*. John Wiley & Sons.

Wilensky, U. (1999). NetLogo. http://ccl.northwestern.edu/netlogo/.

Yolles, Maurice. 2021. "Metacybernetics: Towards a General Theory of Higher Order Cybernetics." *Systems* 9 (2): 34. doi:10.3390/systems9020034.

Zio, Enrico, and Giovanni Sansavini. 2011. "Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins.". *IEEE Transactions on Reliability* 60 (1): 94–101. doi:10.1109/TR.2010.2104211

ANNEX A: PILOT TEST SCENARIO AND TEST CASE

Situation: *The physical results of the presence of emergent behavior in a BMS are goal-seeking elements that may exhibit probabilistic unanticipated behaviors. This is because of a set of input conditions that were unanticipated by the defense doctrine, FPS, and other supporting policy and governance documents for acquisition of assets, or from the adaptation of a person (agent) or software to sets of input rules such as misapplication of the rules by a document and person (agent).*

- *A future soldier system is required to provide an optimized solution for several soldier roles in a variety of mission types. Once this system is integrated into the whole network we are faced with the emergent behavior occurring.*
- *The network needs to allow for future support of an increasing range of sensors and broader field intelligence capabilities. The mesh network is built on a standardized technology platform and supports a set of standard data exchanges based on generic vehicle (GVA) and generic soldier (GSA) architecture models. This allows the SPAN mesh to provide the network for all sensors.*
- *The SPAN mesh at the soldier and section levels is based on leveraging several existing wireless technologies with new and evolving technology to create a low-power mesh network such as Bluetooth/Wi-Fi and/or UWB.*

Test Scenario 1: The CBMS communication system interface and the configuration of the combat network in land forces include wireless networking, sensors, human biosensors, targeting, shot detection, UAVs, small arm digital sights, range finders, and data to consider important issues where an alert/deficiency/loss/failure is experienced due to cyber or electronic warfare attack that has spoofed the BMS system.

- *In this instance, headquarters (HQ) looks at an uncommon BMS program location for something that does not exist; however, another covert operation is being carried out elsewhere.*
- *The ability to remotely monitor the physical condition of each soldier in a dismounted unit is an essential component for the safety, efficiency, and effectiveness of the unit. Why?*
- *A cyber or electronic warfare attack to BMS and network soldier communication network causes data exchange failure. As SPAM is mobile, the section commander, signaler, or vehicle can carry the SPAN transceiver and tactical radio to allow data exchange. Will this capability enhance the positive emergence in SoS?*

Context/Framing Information:

- *SPAN is integrated with the broader army network by connecting it to an existing VHF network, broadband, and future waveforms. By combining some existing radio knowledge with the new SPAN mesh and local higher capacity network, a link is created with the land force backbone network. Will this capability enhance the positive emergence in SoS or will it be destructive?Why?*

Test Cases 1: Australian land forces face limitations in communication capabilities essential for BMS coordination and situation awareness understanding.

- *CBMS rely on the seamless integration of digital and physical components, as well as the possibility of human interactions, which necessitates reliable C4I. Is this seamless integration of digital and physical components feasible? Why?*

- ***Not Covered in this paper** - Automated BMS is used to support human decision-makers. The introduction of the DBM solution (which is the disruptive new technology) may serve to develop suitable automated decision tools to integrate with the BMS command and soldier. Is this technology a good idea and/or is it required?*

ANNEX B: PILOT TEST CASE RESPONSES AND ASSOCIATED CHANGES TO THE CBMS NETWORK SOLDIER DESIGN

Table 1: Pilot Test Case responses and associated with CBMS network soldier

Test Scenario	Test Case	Response	Change to CBMS network soldier Design
Test Scenario 1 – The CBMS communication system interface and in the configuration of the combat network in land forces where wireless networking, sensors, human biosensors, targeting, shot detection, UAVs, small arm digital sights, range finders, and data to consider important issue where an alert/ deficiency/loss/failure is experienced due to cyber or electronic warfare attack, that has spoofed the BMS system.	Test Case 1: Australian land forces may have degradation or lack of communications capabilities essential for BMS coordination and situation awareness understanding.	CBMS rely on the seamless integration of digital and physical components, as well as the possibility of human interactions, which necessitates reliable C4I.? Enabling technologies, such as collections of first-person shooters (FPS) elements s (nodes, vertices) and their pairwise links (edges, connections) and are presented in the simple form of a connection matrix showing positive or negative unexpected emergent behavior in soldier SoS.	The automated BMS is used to support the human decision-makers. The introduction of the DBM solution (which is the disruptive new technology) may serve to develop suitable automated decision tools to integrate with BMS command and soldier. The SPAN solution is an innovative mesh network for sharing data between soldiers in a section, and between commands and sections.

- **Key Findings and Lessons Learned**
  - **Findings**

- Overall, the Pilot successfully tested the applicable elements of the CBMS and network soldier. With the creation of the SPAN mesh, multiple sensors can be fused to create higher-order information. By connecting sensors via mesh networks to a BMS's processing capability, additional algorithms and techniques can be used to combine and analyze network data.

- CBMSs have traditionally combined elements of cybernetics, mechatronics, control theory, systems engineering, embedded systems, sensor networks, data, distributed control, and communications.

  - **Lessons Learned**

Regarding the CBMS and network soldier, we shall consider the use of cybernetics VSM application in meta meta-systems named meta-cybernetics to control variety.

  - **Conclusion**

The Pilot was successful in testing the CBMS network soldier against the professional and experienced personnel and confirmed against the current literature referenced in chapter 4 of this paper.

  - **Recommendations**

As a result of the Pilot, there are key recommendations:

- Use meta-cybernetics in BMS to control variety and reduce negative behaviors.
- Introduce new technology, automated systems that use new logarithms to detect cyberattacks and negative emergent behaviors.
- DBM solution (which is the disruptive new technology) may serve to develop suitable automated decision tools to integrate with the CBMS command and soldier.